Solution Brief
Single Connect Solution

Single Connect Kron

Stronger, Simpler and More Secure Unified Management of Privileged Access Accounts

Single Connect unifies multi-vendor environments with pre-integrated modules managing dozens of vendors and hundreds of network elements with a single, universal system.

In this solution brief, you will learn about the framework for Single Connect and how it enables IT teams in large enterprises to:

- Efficiently secure access to network infrastructure and applications
- Conveniently and universally control configurations
- Comprehensively record all activities in the network and data center that impact business continuity

> **Mastering the solution requires a comprehensive understanding of the challenges.**

Applications

Single Connect addresses:

- Regulatory Compliance
- Risk of insider threats
- Malware that targets privileged accounts
- Security of outsourced IT operations (contractors and vendors)
- Audit trails and on-demand reporting

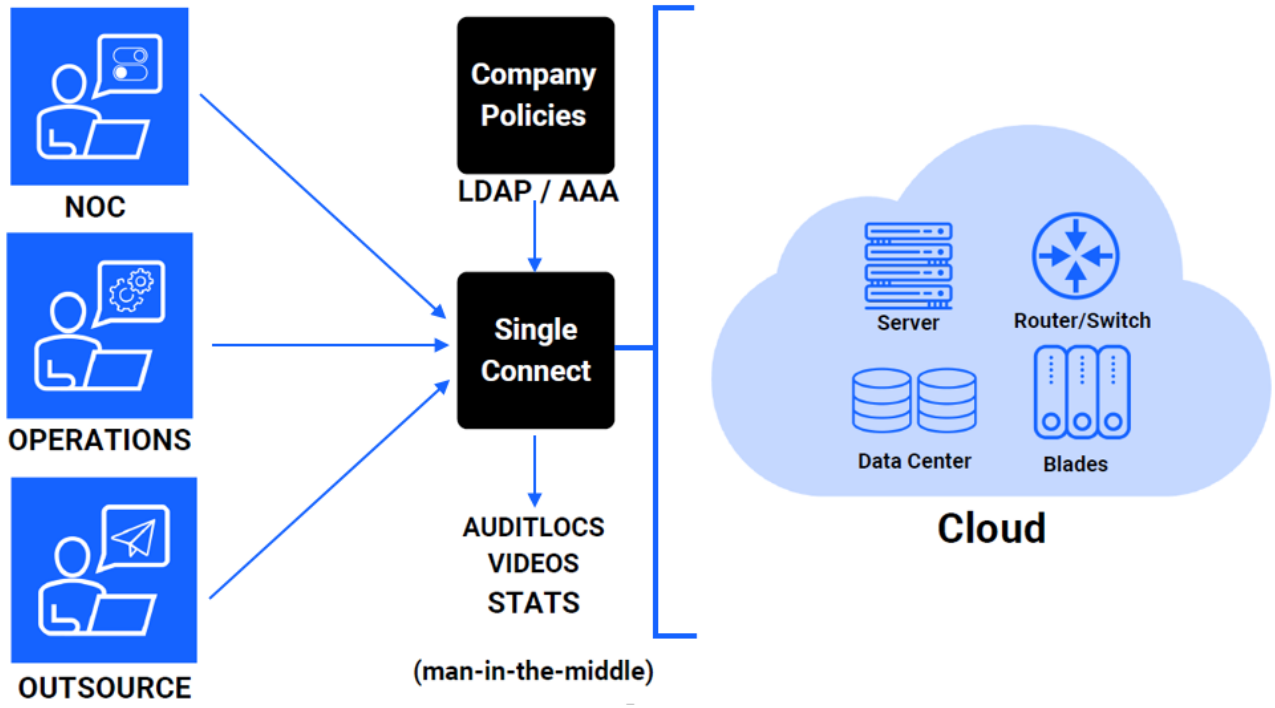
Proven Solution Benefits

Single Connect prevents and detects breaches, maintains individual accountability, and increases operational efficiency significantly by managing credentials and delegating privileged actions.

This proven solution reduces the implementation time required to set up privileged access control compared to other solutions and can scale to support tens of thousands of users and accounts, millions of devices and end-points, and billions of authentication combinations.

Whether applied to real-time communications systems, desktops, mobile devices, and collaboration applications, or to the connected machines as part of the Internet of Things deployments, Single Connect dramatically reduces the complexity associated with a fully effective, fully compliant solution.

High-Level Framework



Solution Features

- Sits in the middle for SSH/HTTP/RDP proxy
- Session management and dual control
- Logging and Session Recording
- Object Character Recognition for RDP, RDP session recording
- Internal Tacacs and Radius support
- Single-Sign-On (SSO)
- Password management, changing password in configurable interval, password history
- Linux/Windows/Network Element Password

Management Capabilities

- Limit / filter command (proxy)
- Multitenancy
- Advanced Policy
- Context Aware Policy
- Multi Factor Authentication with
- GeoFencing
- OTT one-time password for NE

The Triple A's

The principle of controlling which entities are accessing enterprise networks or using network equipment is known as Authentication, Authorization, and Accounting (AAA).

- **Authentication:** Understanding who an entity is before allowing them to perform specific or any actions
- **Authorization:** Ensuring the entity has the privilege to perform the actions
- **Accounting:** Historical and accurate records detailing the actions that have occurred or the resources consumed

The concept of AAA may be applied to many different aspects of a technology lifecycle. However, Device Administration and Network Access are the two main AAA types for networking. The two main AAA protocols commonly used for device administration in enterprise networks today are TACACS+ and RADIUS.

Single Connect manages authentication, authorization, and accounting in a single view, making the management of mixed-vendor networks much less time-consuming, complex, and therefore less expensive.

Single Connect: improving device administration

Controlling access to who can log in to a network device via SSH/TELNET sessions, device administration is very interactive in nature. A user may be authenticated once but may also be required authentication many times during a single session in the command-line of a device, depending on the policy.

Policies that enforce privilege-level and command-set permissions are required. One user may have the privilege to execute only monitoring (read-only) command-set, while another user may have the privilege to change the configuration of devices.

Both RADIUS (Remote Access Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System) can be used for such scenarios. Since TACACS+ can separate authentication, authorization, and accounting as independent functions, it supports a more granular privilege level for device administration.

Single Connect: securing network access through Identity Management

Securing the identity of a user before permitting that user to connect to your network is a mission-critical function for all large enterprises. Both TACACS and RADIUS can be used for this, and Single Connect supports both within the same framework.

Single Connect: pre-Integrated with all major identity databases

Krontech's Single Connect solution integrates all major enterprise identity databases, including Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) databases. Policies can be created based on groups or subgroups which are already configured in these identity databases. Single Connect can enforce user, source address, device type, or date & time-based policies. Built-in integration support to NMS and SIEM systems provides advanced audit capabilities.

Single Connect: no degradation of performance, no hardware complexity

Single Connect features built-in high availability support, granting with Active-Active or Active-Passive mode support, full database synchronization, and geosite redundancy features. Single Connect supports tremendous volumes of concurrent sessions with no degradation in performance. No additional hardware or complexity (such as Fabric Path) is required to support geographic redundancy.

Single Connect: faster, simpler implementation

Single Connect reduces implementation time by approximately 80% compared to other solutions. Single Connect is proven to scale up to millions of devices, tens of thousands of users and automated accounts, and billions of authentication combinations.

Throughout, Single Connect reduces the complexity of maintaining Privileged Access security with an agentless “man in the middle” approach.

Single Connect was developed based on market research and in collaboration with some of the largest enterprises and telecom service providers in the world, with hundreds of implementations already in place and new implementations happening every month.

What IT Teams Do with Single Connect

- Secure, centralize and automate the management of passwords for administrative, service, and application accounts, as well as enforcement of password policies
- Control access to shared accounts
- Manage and monitor privileged sessions, commands, and actions in real-time, recording them for audit and other purposes
- Control and filter commands or actions a system user can execute
- Provide superuser capabilities for managing administrative access
- Keep a detailed view of privileged accounts and capabilities for different kinds of visualization such as dashboards and reporting

Single Connect integrates easily with other Krontech products and third-party systems, enhancing those systems, simplifying change management workflows, and substantially strengthening compliance and audit capabilities through greater automation.

Policy-based automation and management: four main modules

Krontech's Single Connect system is based on four main modules: Session Manager, Password Manager, 2FA Manager, TACACS Access Manager.

Session Manager	Password Manager	2FA Manager	TACACS Access Manager
Logging and recording all sessions, including command and context-aware filtering	More efficiency and security for admins and operators with shared account password management features	A second layer of authentication through integration between desktop and mobile security	Terminal Access Controller Access Control System Plus (TACACS+) protocol-based security software

- Person in the middle scenario for SSH/HTTP/RDP proxy
- Session management and dual control
- Logging and Session Recording
- Object Character Recognition for RDP, RDP session recording
- Internal Tacacs and Radius support
- Single-Sign-On (SSO)
- Password management, changing password in the configurable interval, Password history
- Break Glass
- Linux/Windows/Network Element Password Management
- Limit/filter command (proxy)
- Multitenancy
- Advanced Policy
- Context-Aware Policy
- Multi-Factor Authentication with GeoFencing

Distributed Architecture

Due to its distributed architecture, Krontech's Single Connect features built-in high availability support, granting with Active-Active or Active-Passive mode support, full database synchronization, and geosite redundancy features.

Flexible Deployment Models

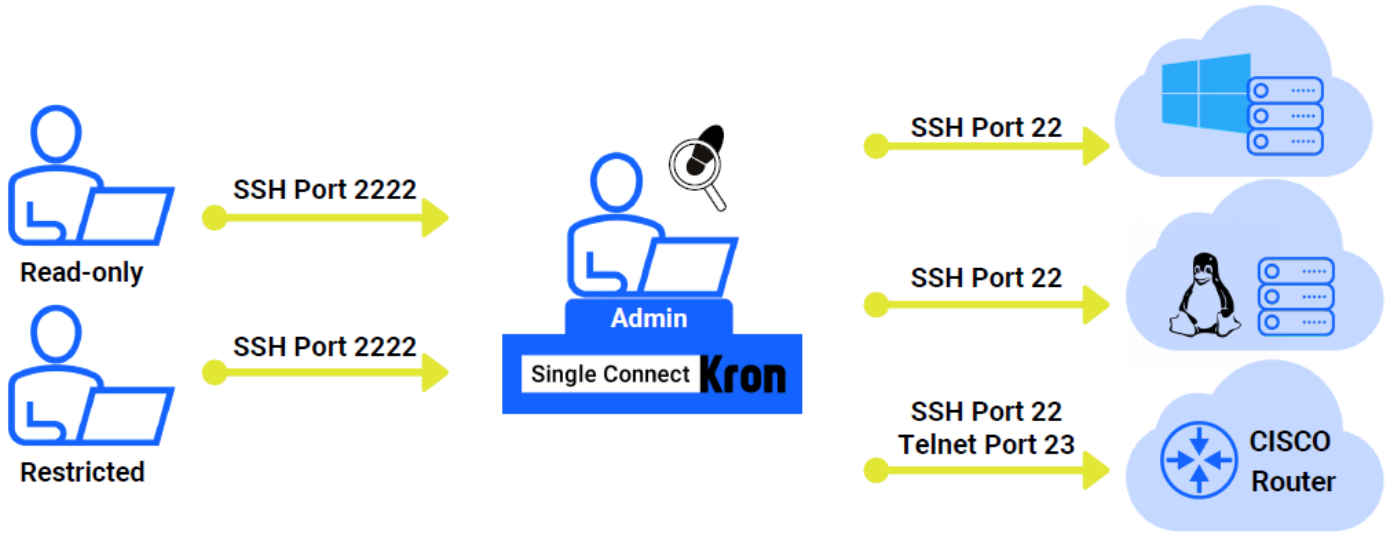
Single Connect can run on its special purpose-built appliance or on a virtual machine in the cloud.

Easy to Configure

The scenario below illustrates how flexible the Single Connect solution is.
This scenario consists of sample users, devices, and policy definitions. There are three types of users and three types of devices in this scenario:

User Types	Device Types
1. Restricted 2. Read-only 3. Administrator	1. Linux 2. Windows 3. Cisco

Policy keys are defined within as restricted, read-only, permit-all, confirmation, and approval policy groups and assigned to related user and device groups accordingly.



Single Connect GUI

Logging into Single Connect

Users can log in to Single Connect with a password for the first time and immediately reset their personal password after initial login.

More detailed information about Krontech's Single Connect technology is available on request through detailed user manuals and workflow documentation